Countermeasures for GPS signal spoofing

Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal and John Fagan
The University of Oklahoma

BIOGRAPHY

Hengqing Wen is Research Associate at the University of Oklahoma. He has been involved in FAA-sponsored WAAS and LAAS flight test projects since 1999 and participated in the design, development and test of the LAAS system at the university airport. Mr. Wen's research interests include LAAS and WAAS navigation, signal processing, wireless communication, and LAAS implementation. He is currently researching interference of the LAAS VHF link and is playing a major role in building a certifiable LAAS.

Peter Yih-Ru Huang is a Research Associate in the Department of Electrical and Computer Engineering at the University of Oklahoma and received his MS degree in 2004. He joined the FAA LAAS project in 2001 and finished many flight and ground test analysis for LAAS and GPS. Peter's areas of expertise are WAAS/LAAS navigation, GPS truth system, and system statistical analysis. Peter is working on his PhD degree and continues to participate in the design and implementation of a certified LAAS.

John Dyer is Research Associate at the University of Oklahoma. John is currently working on his PhD in the Department of Electrical and Computer Engineering. His past research has involved algorithm development for digital signal processing in the biomedical arena. Currently, his research involves GPS signal dynamics within the LAAS environment.

Andy Archinal is a Research Associate at the University of Oklahoma. He has been involved in FAA sponsored LAAS and Curved Path flight test projects since 2000. His past research has included the development and testing of the OU Curved Path Navigator and Crew Chief of the OU Formula Lightning race car. Currently his research involves LAAS integrity monitoring and LAAS complex approach procedures.

John Fagan serves as Presidential Professor of Electrical and Computer Engineering at the University of Oklahoma. He is an active teacher and researcher in the area of alternate energy transportation systems, and the use of GPS as an aircraft landing and navigation tool. Dr. Fagan works with the FAA and the OU Department of Aviation to help determine the use of GPS, WAAS and LAAS for precision and non-precision approach procedures in the terminal arrival area. John has worked as the principal investigator on a flight test program for category A and B aircraft using the WAAS and the LAAS navigator system for precision approaches as well as a test program for the C-129 GPS navigators.

ABSTRACT

The strength of the GPS signal on the earth's surface averages -160 dBw . While many GPS receivers leave large space for signal dynamics, enough power space is left for the GPS signals to be overridden (spoofed). Spoofing is completely different from jamming. The objective of jamming is to simply interrupt the availability of the signal in space at the receiver. The effect is to cause the signal at the receiver to be corrupted so that no valid GPS signal can be decoded by the receiver. The goal of spoofing, on the other hand, is to provide the receiver with a misleading signal, fooling the receiver to use fake signals in space for positioning calculations. The receiver will produce a misleading position solution. While the GPS P-code is heavily encrypted and thus, is hard to spoof, the civilian GPS signal, the C/A code, is easy to spoof because the signal structure, the spread spectrum codes, and modulation methods are open to the public. The purpose of this paper is to analyze the vulnerability of the satellite signal and GPS system to spoof attacks, propose the anti-spoofing algorithms and illustrate the simulations of spoofing impact and anti-spoofing results. It is believed by the authors of this paper that GPS can be spoofed in theory and producing a spoofing satellite signal is possible. However, practical spoofing that provides misleading navigation results at the receiver is difficult to conduct due to the signal infrastructure, and by applying trivial anti-spoofing algorithms in GPS receivers, spoofing attack can be easily detected.

INTRODUCTION

In this paper, we are going to present anti-spoof research on the GPS signal in space. For purposes of discussion, a spoof is defined as a malicious signal that overpowers the authentic signal and misleads the receiver to use a forged signal for further processing. Figure 1 is a general block diagram of a GPS receiver. Most receivers are equipped with an automatic gain control (AGC) that adjusts the gain of the front-end amplifier so that the A/D converter can use its full range operation without saturation or under range. AGC plays an important role in a successful spoof.

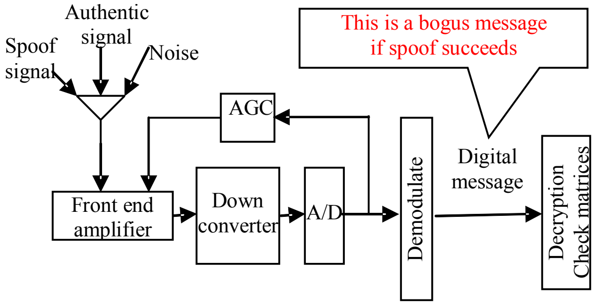

Figure 1 AGC and spoof vulnerability

The composite signal received at the antenna is

$$S_{ant} = S_a + S_s + S_N \,. \qquad (1)$$

where S_a is the authentic signal, and S_s is the spoof signal. When

$$S_s >> S_a \,, \qquad (2)$$

the signal received at the antenna can be approximated by $S_{ant} \approx S_s + S_N$. At the A/D sampler, spoof data are decoded and the spoof signal successfully overrides the authentic signal. Only after the signal is decoded into digital format can the decryption and check matrix tests be conducted. Therefore, as long as the algorithms for encryption and check matrices are accessible to the public, they cannot be used to detect spoof attacks, because spoof messages can employ the correct algorithm so that they appear authentic to the receiver. Spoofing is more serious than jamming because jamming will cause the service to degrade in performance while spoofing takes control of the user receiver.

This paper will discuss the spoof and anti-spoof issue on a single antenna GPS receiver only. However, the countermeasures proposed are also applicable to receivers with an antenna array. We will discuss spoofing in more detail and present countermeasures.

GPS SIGNAL WAVEFORMS

The GPS L1 carrier is modulated with the in-phase and quadrature components as expressed in (3) and (4) as

$$I_{L1}(t) = a_{I1}P(t)W(t)D(t)\cos(f_1 t) \qquad (3)$$

$$Q_{L1}(t) = a_{Q1}C\_A(t)D(t)\sin(f_1 t)\,, \qquad (4)$$

where *D(t)* is the GPS message whose format is published in the GPS ICD , *P(t)* is the P-code, *C_A(t)* is the C/A code, *W(t)* is the W-code that encodes P-code into Y-code when GPS anti-spoof is turned on, and a_{I1} and a_{Q1} are the signal amplitudes for in-phase and quadrature, respectively. Assume that the L2 frequency is modulated with Y-code only (un-modernized GPS), then the waveform on the L2 carrier is

$$L2(t) = a_2 P(t)W(t)D(t)\cos(f_2 t)\,, \qquad (5)$$

where a_2 is the signal amplitude.

Seen from equations (3) - (5), except the W-code, all the elements of the GPS waveforms can be pre-programmed, i.e., GPS waveforms can be forged when GPS anti-spoof is off. At least we can see here, the authentic C/A signal on L1 carrier can be overridden and thus the GPS message can be spoofed if a signal generates a waveform of (4) and a_{Q1} is chosen to satisfy (2). However, message spoofing alone is not sufficient to conduct a successful spoof attack because only after a receiver reaches erroneous solutions on position, velocity and time, can one say it is a successful spoof. Other GPS observables are also affecting the GPS solution.

SPOOFING VULNERABILITY

There are four GPS observables that can be directly measured by a GPS receiver. They are the GPS message, code ranges, fractional phase ranges and Doppler shift. These observables will be studied one by one to estimate the vulnerability.

In a GPS receiver, PRN code correlation is performed at high frequency to remove the PRN code. The received GPS signal is passed through a high pass filter to remove navigation data. After the navigation message is removed, the resulting signal is the Doppler shifted carrier. The Doppler shifted carrier is then passed to a PLL and compared with a receiver-generated carrier to get the fractional phase offset.

The GPS message is derived after PRN code correlation. In the navigation message, HOW in each subframe tells how to track P-code. As analyzed above, the GPS message can be spoofed because PRN code is available to the public.

The PRN code ranges of C/A code and P-code are direct observables. One chip of C/A code range will cause 300 km ambiguity. The range measurement for C/A code is the basic observation of GPS receivers and it is derived from the time shift of the receiver PRN sequence and the PRN sequence that is multiplexing the incoming signal. This time shift, however, can be controlled by spoofing the transmitter. Pseudorange measurements can be modeled as

$$\rho_i = \left|r_i - r_u\right| + c \cdot b_u \;| + \varepsilon_{\rho_i}\,, \qquad (6)$$

where i is the satellite index; r_i is the satellite position at transmit time; r_u is the receiver position at receive time; b_u is the receiver clock bias and ε_ρ is the composite of various errors. The satellite position vector r_i can be forged by spoofing the GPS messages. Using this model, the PRN code shift can be easily calculated. Spoofing a static receiver is much easier than spoofing a dynamic receiver. For a stationary receiver, the position solution is fixed; the spoofed pseudorange can be calculated using code range model (6). For a moving receiver, if the spoofer does not need to avoid cross-checking at the spoofed receiver, then the position solution can be forged in advance and then use (6) again to get a time sequence of the spoofed pseudorange. Waveform (7) is a bogus version of waveform (4), where the quantities with prime (′) are forged by the spoofer and τ is the time shift intentionally added to the spoof signal.

$$Q'_{L1}(t) = a'_{Q1} C\_A(t-\tau) D'(t)\sin(f_1 t) \qquad (7)$$

The fractional phase ranges for L1 and L2 are direct observables. Integer ambiguity however, is not, because it's computed using some kind of algorithm. Moving one step further from (7) we get a forged GPS signal with spoofed C/A code range and spoofed C/A carrier phase as

$$Q''_{L1}(t) = a'_{Q1} C\_A(t-\tau) D'(t)\sin(f_1 t + \Phi'). \qquad (8)$$

A ~~doppler~~Doppler observation is the output of phase locked loop (PLL) after the frequency down converter. The actual measured carrier frequency is

$$f' = f_0/(1+v/c), \qquad (9)$$

where f_0 is the nominal frequency, c is the speed of light and v is the velocity of satellite with respect to the receiver antenna. Velocity v is positive if the satellite is moving away from observer and negative if the source is moving towards the observer. Another step ahead from (8) is (10).

$$Q'''_{L1}(t) = a'_{Q1} C\_A(t-\tau) D'(t)\sin((f_1 + \Delta f')t + \Phi') \qquad (10)$$

The signal expressed in (10) is a spoof signal with strong carrier power to override the authentic GPS signal, modulated with a forged GPS message and time shifted PRN code, and phase shifted L1 carrier. Thus, the RF signal in space is generated and the timing can be controlled. A waveform expressed by (10) forges all the GPS observables and one such signal source can spoof all the GPS observables related to the C/A code on the L1 frequency from one satellite.

Similarly, the in-phase component of L1 and the component on L2 expressed in (3) and (5), respectively, can be forged in the same way.

The GPS message and code range are fundamental measurements in any GPS receiver. These two observables are easy to forge. Therefore, spoofing a C/A code receiver is much easier than spoofing an L1/L2 receiver. Even though only these two observables are spoofed, the phase range measurements will be affected and the L1/L2 carrier differential calculation will also be affected. Doppler shift measurements are not used for the position solution by most GPS receivers.

Intentional jamming signals usually try to disable the GPS signal. Spatial volume and duration are criteria for successful jamming. Spoofing, on the other hand, is not concerned with spatial volume. It is always object oriented. It might be aiming at only one specific receiver for a very short time.

Although GPS antennas on airplanes are omni-directional antennas with null pointing downward, and thus, unlikely to be affected by a ground based spoof source, directional antennas with enough power output can still override the authentic GPS signal.

THE POWER TO SPOOF

In practice, the actual power needed to spoof is not required to satisfy (2). Referring to Figure 2, consider the GPS signal modulation. On the BPSK constellation, there are only two symbols, A and B, and their power is normalized such that symbol power strength is 1. The 2D constellation is divided into two decision regions: to the left of the origin is the decision region for symbol A and to the right of the origin is the decision region for symbol B. Now consider a spoof signal with symbols A' and B' with

$$\|OA'\|=\|OB'\|\geq 1. \qquad (11)$$

If the noise is not considered, the spoof power required to pull symbols A and B into the decision region of A' is 1 and the power required to pull both symbols to the B' decision region is also 1. In other words, if noise is not considered, the required power to spoof the authentic BPSK signal is exactly the authentic signal power. When noise is considered, the required spoof power is

$$\|OA'\|=\|OB'\|\geq 1+N_c, \qquad (12)$$

where N_c is the overall channel noise that includes the noise incurred at satellite, in space, multipath, other interference and receiver noise. Noise N_c is also normalized by the authentic symbol power. Condition (12) says that if the received spoof signal power is greater than the received authentic signal power plus the noise power, the authentic signal will be overridden and the receiver will decode the message on the spoof carrier. The requirement described by (12) is for spoofing the GPS message from one satellite only.

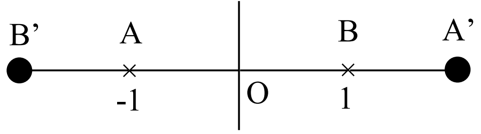

Figure 2 BPSK symbol constellation.

COUNTERMEASURES

As a one-way broadcast system, GPS is not immune to spoof attack except the Y-code whose encryption algorithm is not available to civilian users. As analyzed in the introduction section, a spoof can never be detected using check matrices, like the CRC check, in the digital domain. However, by cross-checking the observables, intermediate measurement, and positioning solutions, a spoof can be detected.

This paper will consider only spoof detection methods for stand alone GPS receivers for ordinary civilian users. We will discuss the prospective self-check algorithms in the GPS receiver. Differential GPS can easily detect a spoof presence at a rover. However, the methods to detect a spoof in a differential system are not to be discussed in this paper. Special antenna design and cross-checking with other observations, like inertial system, will not be studied here either.

Method 1. *Monitor the absolute power of each carrier*
According to , the received signal power is not expected to exceed -155.5 dBw and -153dBw, respectively for P(Y) code and C/A code components of the L1 channel, nor -158 dBw for either signal on the L2 channel. These numbers do not set the upper limit of signal power for every receiver because antenna type and attitude, and environmental effects like multipath may change the received signal power dramatically. Nevertheless, a reasonable maximum power can be set to limit the spoof signal power in space, because a spoof station will increase the signal power in space by at least 3 dB.

Method 2. *Monitor Signal power changing rate*
RF signal radiating from a point source satisfies

$$Pr^2 = \text{constant}, \qquad (13)$$

where P is the received power and r is the distance between satellite and receiver. Since GPS satellites are 20,000 km away from earth, any position change near earth's surface should not change signal power dramatically. However, since received power is deeply dependent on the environment, like multipath and antenna attitude, this method only applies to static observations. Meanwhile, since the elevation of a satellite affects received signal power, this method can be used in time intervals when satellite elevation remains constant. The signal to noise ratio that is available in most GPS receivers can be used to take the place of P in equation (13).

Method 3. *Monitor the relative powers*
Reference gives the minimum received RF signal power strength on L1 frequency as -163.0dBW for P(Y) code and -160dBW for C/A code. The minimum signal power strength on L2 frequency is -166dBW. The 3dB step is the underlying relation in setting up the reasonable power ratios. Modernized GPS will have two signals on L2 and one signal on L5. These signals will also have relatively fixed power ratios. On checking the relative power ratio, those types of spoof that do not override all of the signal components on all frequencies (L1/L2 and modernized L5) can be easily detected. The advantage of this method is that it is not affected by antenna attitude. However, ionosphere refraction may affect the power ratio on different frequencies.

Method 4. *Bound and compare range rates*
We define range rate here as the rate at which the code/phase range measurement changes, i.e.

$$RR_{code} = (r_i - r_j)/(t_i - t_j), \qquad (14)$$

$$RR_{phase} = \int_{t_{ji}}^{t_i} \Phi(t)dt/(t_i - t_j), \qquad (15)$$

where i and j are observation index, r is the code range observation, Φ is the fractional phase measurement and t is the observation time. Although a spoofer can easily spoof the phase measurement at a static receiver, a moving receiver's phase measurement is not under the spoofer's control. In order to spoof a receiver, code range must be spoofed properly and phase ranges have to be spoofed in accordance with code range if a spoofer wants to let phase range conform to code range. When phase ranges are to be forged with respect to code range, phase range rate will probably be sacrificed to spoof phase range. Therefore, comparing code and phase range rates can detect the abnormality, and bounding the rates gives a mechanism to detect the abnormality. The range rate with respect to GPS satellites cannot be even comparable to the range rate measured from the spoof signal that is transmitted from ground-based transmitter.

Method 5. *Doppler shift check*
GPS receivers have position solution and satellite position. The relative speed of the receiver with respect to each GPS satellite can thus be derived. The Doppler shift derived from (9) can be

$$D = f' - f_0 = -f_0/(1 + c/v). \qquad (16)$$

It is impossible to get all the Doppler shifts for all satellites correct by mimicking satellite movement by the spoof source using a single transmitter because the Doppler shift is changing carrier frequency. Although CDMA signals with different PRN code can be summed before being modulated on a carrier, the spoof signal has to be modulated to a different carrier to avoid the Doppler test. A spoofer might thus have to use one transmitter for each spoofed SV. The Doppler shift should also compare with the range rates because it has internal relation with phase range rate, i.e.

$$D = \lambda \dot{\Phi} \qquad (17)$$

Method 6. *Cross-correlation of L1 and L2*

Cross-correlation is a codeless technique , ~~i.e~~i.e., it does not need knowledge about the code. L1 is modulated with the C/A code and the P(Y) code, (non-modernized). L2 has either the C/A code or the P(Y) and practically L2 is modulated with P(Y) code. If we assume at least one of the codes on L1 is identical to the code on L2 and assume the code is the P(Y) code, then, the cross-correlation between the identical signals on L1 and L2 will generate one peak only, because the P-code length has the period of one week. Since the signal on L2 is slower than that on L1 due to ionosphere effect, the sign of cross-correlation shift is known. Even though the Y-code is turned on, GPS receivers with a built-in P-code correlator can also do this test because $f_Y = f_P = 20 f_W$ and there exist segments in the Y-code data streams that are identical to its counterpart P-code. This test requires spoofers to spoof both carriers if any L1 or L2 carrier is spoofed, i.e. messages on both carriers must be spoofed.

Method 7. *Residual analysis*

The received signal under spoof attack consists of three components—the spoofed signal, the attenuated authentic signal and comprehensive noise. If we consider only one satellite signal, the received signal shown in (18) is

$$S_r = S_S + kS_A + N_T . \qquad (18)$$

where S_r is received signal, S_S is spoof signal, S_A is the authentic signal and k is the strength ratio of authentic signal to spoof signal. After the spoof GPS message is removed, the residual signal will consist of the authentic signal that might be decoded. However, this is not guaranteed because the ratio of spoofed power to authentic signal power determines the attenuation gain k. If the attenuation is too strong, the authentic signal is not recoverable.

Method 8. *L1-L2 range differences*

The range measurements from L1 and L2 can be related as

$$R_{L2} = R_{L1,C/A} + (R_{L2,Y} - R_{L1,Y}) \qquad (19)$$

$$\Phi_{L2} = \Phi_{L1,C/A} + (\Phi_{L2} - \Phi_{L1}) . \qquad (20)$$

Range differences between L1 and L2 are caused by ionosphere effects. Phase and code ranges should conform to each other. The spoofed signal that is propagating only in the lower layer of atmosphere behaves differently in (19) and (20) from the authentic signal with ionosphere delay. A ground-based transmitter usually gives a good conformity between L1 and L2 range measurements.

Method 9. *Verify received ephemeris data*

Compare received ephemeris data that will be used to calculate satellite position with known non-spoofed ephemeris and almanac data to ensure that the received GPS message does not provide fixed satellite information and no SV position is too far away from the almanac position. This test will make sure that the spoofer cannot use its own position as a satellite position. This is a protection for and .

Method 10. *Jump detection*

All observables should monitor abrupt changes in the observables and power within a tolerable range. Any jump in observables or signal power might mean the turning on of a spoof attack. For receivers that pass through a very large distance, it is quite likely it will move from a non-spoofed area into spoofed area. In between, there must be an area that the receiver cannot decode a valid GPS message because a 3 dB signal power change requires a spatial change. If the spoofer does not want the receiver to experience this "no message" state, a sudden power overriding is needed for the spoof transmitter to override the authentic signal. Both the signal power and navigation message should be checked.

SUMMARY OF COUNTERMEASURES

For the sake of the clarity, these countermeasures are summarized in Table 1.

Method	Test statistic	Function	Limitation
	Absolute signal power	Limit the spoof signal power	Antenna attitude and environment related
	Signal power changing rate	Detect stationary spoof station	Antenna attitude and environment related
	Relative signal strengths on all carriers	Detect spoofing on single carrier	Affected by ionosphere refraction
	Range rate	Bound the phase and code range rate	Relate to GPS receiver's moving direction
	Doppler shift	Detect spoof that uses one transmitter to spoof all satellites	None
	Correlation peaks	Correlate L1/L2 binary message	Low performance on Y-code
	GPS signal after removing all navigation data	Recover authentic data	Requires low spoof/authentic signal power ratio
	Range differences: phase/code, L1/L2	Identify signal source	Needs to be L1/L2 receiver
	Ephemeris data	Verify ephemeris data including satellite position	None
	Signal power and data	Jump detection	None

Table 1 Summary of anti-spoof methods.

CONCLUSSION

This paper discussed the vulnerability of a single GPS receiver to a spoof attack in detail and presented, in general view, the methods for anti-spoof. These methods use intermediate signals to detect the presence of a spoof attack. In this paper we only discussed those methods that can be processed in software without modification of the receiver design. These software methods are trivial because most of them are using intermediate measurements directly available in GPS receivers. These methods are not stand-alone and they support each other to fulfill the whole anti-spoof task. For example, if the absolute power is not limited (), the residual test () will not function properly; if the ephemeris data is not verified () a spoofed GPS message can simply use its real position as the satellite position and thus, the phase measurement will look legitimate and will fail. Due to the time constraint, we did not provide details for these methods. Some of the major algorithms and parameters/thresholds used will be discussed in later papers.

As a result of this research, we believe that a GPS spoof is not formidable because it can be detected very easily and the authentic signal can be recovered in some cases. However, if nothing is done, the GPS receiver is vulnerable to spoof attack.

ACKNOWLEDGMENTS

This research is undertaken with the help of the Leading Edge Navigation System, a company based in Norman, Oklahoma.

REFERENCES

[1] J. S. Warner and R. G. Johnston, December 2003, *GPS Spoofing Countermeasures*, http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html

[2] B. W. Parkinson and J. J. Spiker Jr., 1996, *Global Positioning System: Theory and Applications*, American Institute of Aeronautics and Astronautics, Inc.

[3] B. Hofmann-Wellenhof, H. Lichtenegger and J. Collins, *GPS Theory and Practice*, fifth edition, SpringerWien New York, 2001.

[4] A. Leick, *GPS Sattellite Surveying*, John Wiley & Sons, Inc, 2004.

[5] Department of Defense. (2000). *Navstar GPS Space Segment/Navigation User Interfaces* (*ICD-GPS-200C with IRN-200C-004*), 12 April 2000. Washington, DC: U.S. Government Printing Office. http://www.navcen.uscg.gov/pubs/gps/icd200/icd200cw1234.pdf